Attacks on Implementations of Secure Systems

August 6, 2019

Contents

Foreword

This document contains the collected scribe notes created by the students of my course titled "Attacks on Secure Implementations", given in Ben-Gurion University during Spring 2019.

The following students contributed to the writing process:

- **Chapter 1: Introduction.** Transcription by Michal Hershkoviz, graphics by Shir Frumerman, editing by Yoni Tsionov.
- **Chapter 2: Temporal Side-Channels 1.** Transcription by Sagi Nakash, graphics by Ziv Tomarov, editing by Shaked Delarea.
- **Chapter 3: Temporal Side-Channels 2.** Transcription by Itay Rosh, graphics by Noga Agmon, editing by Boris Kazarski.
- **Chapter 4: Low Data Complexity Power/EM 1.** Transcription by Ronen Haber and Rotem Yoeli, graphics by Idan Mosseri, editing by Ben Hasson.
- **Chapter 5: Low Data Complexity Power/EM 2.** Transcription by Barak Davidovich, graphics by Dan Dvorin, editing by Omri Fichman. Section about Template Attacks written by Adnan Jaber.
- **Chapter 6: High Data Complexity Power/EM 1.** Transcription by Vitaly Dyadyuk, graphics by Alon Freund, editing by Omer Nizri.

The text for chapters 1 to 4 is based on lecture notes in Hebrew originally created by Yael Mathov. Tom Mahler was responsible for creating the chapter templates and masterminding the entire editing process. I am grateful to them and to everybody who contributed to this document.

Bibliography

[1] Us navy crypto equipment - 1950's-60's. http://www.navy-radio.com/crypto.htm.

[2] Ryan Singel. Declassified nsa document reveals the secret history of tempest. https://www.wired.com/2008/04/nsa-releases-se/.

[3] memcmp(3) - linux man page. https://linux.die.net/man/3/memcmp.

[4] Flavio D Garcia, Gerhard de Koning Gans, Ruben Muijrers, Peter Van Rossum, Roel Verdult, Ronny Wichers Schreur, and Bart Jacobs. Dismantling mifare classic. In *European symposium on research in computer security*, pages 97–114. Springer, 2008.

[5] Nicolas Courtois, Karsten Nohl, and Sean O'Neil. Algebraic attacks on the crypto-1 stream cipher in mifare classic and oyster cards. *IACR Cryptology ePrint Archive*, 2008:166, 2008.

[6] Signal amplification relay attack (sara). https://hackernoon.com/signal-amplification-relay-attack-sara-609ce6c20d4f.

[7] What is an fpga? https://www.xilinx.com/products/silicon-devices/fpga/what-is-an-fpga.html.

[8] Amir Moradi, Alessandro Barenghi, Timo Kasper, and Christof Paar. On the vulnerability of fpga bitstream encryption against power analysis attacks: extracting

keys from xilinx virtex-ii fpgas. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 111–124. ACM, 2011.

[9] Confidentiality, integrity, and availability. https://developer.mozilla.org/en-US/docs/Web/Security/Information_Security_Basics/Confidentiality,_Integrity,_and_Availability.

[10] Hsiao-Ying Lin and Wen-Guey Tzeng. An efficient solution to the millionaires' problem based on homomorphic encryption. In *International Conference on Applied Cryptography and Network Security*, pages 456–466. Springer, 2005.

[11] Paul C Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In *Annual International Cryptology Conference*, pages 104–113. Springer, 1996.

[12] Atm card blocked after certain numbers of wrong pin.

[13] Burt Kaliski. The mathematics of the rsa public-key cryptosystem. *RSA Laboratories*, 2006.

[14] Wikipedia. Rsa (cryptosystem), 2019.

[15] Jonathan Katz, Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 1996.

[16] Pei Dingyi, Salomaa Arto, and Ding Cunsheng. *Chinese remainder theorem: applications in computing, coding, cryptography*. World Scientific, 1996.

[17] Henry S Warren. *Hacker's delight*. Pearson Education, 2013.

[18] Jean-Francois Dhem, Francois Koeune, Philippe-Alexandre Leroux, Patrick Mestré, Jean-Jacques

Quisquater, and Jean-Louis Willems. A practical implementation of the timing attack. In *International Conference on Smart Card Research and Advanced Applications*, pages 167–182. Springer, 1998.

[19] Wikipedia. Student's t-test, 2019.

[20] Wikipedia. William sealy gosset, 2019.

[21] Marc F Witteman, Jasper GJ van Woudenberg, and Federico Menarini. Defeating rsa multiply-always and message blinding countermeasures. In *Cryptographers' Track at the RSA Conference*, pages 77–88. Springer, 2011.

[22] K. Shirriff. Ken shirriff's blog. http://www.righto.com/2013/09/intel-x86-documentation-has-more-pages.html.

[23] Colin Percival. Cache missing for fun and profit. *BSDCan 2005*, 2005.

[24] Gabriele Paoloni. How to benchmark code execution times on intel® ia-32 and ia-64 instruction set architectures. *White Paper*, 2010.

[25] David Gullasch, Endre Bangerter, and Stephan Krenn. Cache games – bringing access-based cache attacks on aes to practice. In *Proceedings of the 2011 IEEE Symposium on Security and Privacy*, SP '11, pages 490–505, Washington, DC, USA, 2011. IEEE Computer Society.

[26] Dag Arne Osvik, Adi Shamir, and Eran Tromer. Cache attacks and countermeasures: The case of aes. In *Proceedings of the 2006 The Cryptographers' Track at the RSA Conference on Topics in Cryptology*, CT-RSA'06, pages 1–20, Berlin, Heidelberg, 2006. Springer-Verlag.

[27] Falkner Yarom. Flush+reload: a high resolution, low noise, l3 cache side-channel attack. *23rd USENIX Security Symposium*, 2014.

[28] Fangfei Liu, Yuval Yarom, Qian Ge, Gernot Heiser, and Ruby B. Lee. Last-level cache side-channel attacks are practical. In *Proceedings of the 2015 IEEE Symposium on Security and Privacy*, SP '15, pages 605–622, Washington, DC, USA, 2015. IEEE Computer Society.

[29] Clémentine Maurice, Nicolas Le Scouarnec, Christoph Neumann, Olivier Heen, and Aurélien Francillon. Reverse engineering intel last-level cache complex addressing using performance counters. In Herbert Bos, Fabian Monrose, and Gregory Blanc, editors, *Research in Attacks, Intrusions, and Defenses - 18th International Symposium, RAID 2015, Kyoto, Japan, November 2-4, 2015, Proceedings*, volume 9404 of *Lecture Notes in Computer Science*, pages 48–65. Springer, 2015.

[30] C. Maurice. Cache template attacks. https://github.com/clementine-m/cache_template_attacks.

[31] Mangard Gruss, Spreitzer. Cache template attacks: Automating attacks on inclusive last-level caches. *24th USENIX Security Symposium*, 2015.

[32] D. Gruss. Cache template attacks. https://github.com/IAIK/cache_template_attacks.

[33] Hamming weight. https://en.wikipedia.org/wiki/Hamming_weight.

[34] https://en.wikipedia.org/wiki/Pearson_correlation_coefficient.

[35] K. Nohl et al. Reverse-engineering a cryptographic rfid tag. In *17th USENIX Security Symposium*, volume 17. USENIX, 2008. Online; https://www.usenix.org/legacy/events/sec08/tech/full_papers/nohl/nohl.pdf.

[36] A. Govindavajhala, S. & Appel. Using memoryerrors to attack a virtual machine. Princeton University. Online; https://www.cs.princeton.edu/~appel/papers/memerr.pdf.

[37] CHDK Wiki. Obtaining a firmware dump. CHDK Wiki. Online; https://chdk.fandom.com/wiki/Obtaining_a_firmware_dump#Q._How_can_I_get_a_firmware_dump.3F.

[38] HackingHood. Canon sd300 camera analysis. HackingHood. Online; https://sites.google.com/site/hackinghood2/home.

[39] D. Boneh et al. On the importance of eliminating errors in cryptographic computations. Dept. of Computer Science, Stanford University. Online; https://link.springer.com/content/pdf/10.1007/s001450010016.pdf.

[40] M. Joye et al. Chinese remaindering based cryptosystems in the presence of faults. UCL Crypto Group, Dep. de Mathematique, Universite de Louvain. Online; http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.55.5491&rep=rep1&type=pdf.

[41] Schmidt J.M. & Hutter M. Optical and em fault-attacks on crt-based rsa: Concrete results. Institute for Applied Information Processing and Communciations, Graz University of Technology. Online; https://online.tugraz.at/tug_online/voe_main2.getvolltext?pCurrPk=32877.

[42] Y. Kim et al. Flipping bits in memory without accessing them: An experimental study of dram disturbance errors. Intel Labs, Carnegie Mellon University. Online; https://users.ece.cmu.edu/~yoonguk/papers/kim-isca14.pdf.

[43] K. Razavi et al. Flip feng shui: Hammering a needle in the software stack. Vrije Universiteit Amsterdam. Online; https://www.cs.vu.nl/~herbertb/download/papers/flip-feng-shui_bheu16.pdf.

[44] L. Cojocar et al. Exploiting correcting codes: On the effectiveness of ecc memory against rowhammer attacks. Vrije Universiteit Amsterdam. Online; https://cs.vu.nl/~lcr220/ecc/ecc-rh-paper-sp2019-cr.pdf.

[45] CVE-2017-0144. Available from MITRE, CVE-ID CVE-2017-0144. Online; https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144.

[46] Coordinated vulnerability disclosure. Online; https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW5Alv.

[47] Clemens Lode. *Philosophy for Heroes: Knowledge*. Clemens Lode Verlag e.K., 2016.

[48] Clemens Lode. *Philosophy for Heroes: Continuum*. Clemens Lode Verlag e.K., 2017.